NO. 21-55768

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

NORA PHILLIPS; ERIKA PINHEIRO; NATHANIEL DENNISON,

PLAINTIFFS-APPELLANTS,

v.

U.S. CUSTOMS AND BORDER PROTECTION; MARK MORGAN; UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT; MATTHEW ALBENCE; FEDERAL BUREAU OF INVESTIGATION; CHRISTOPHER WRAY,

DEFENDANTS-APPELLEES

On Appeal from the United States District Court
for the Central District of California
2:19-cv-06338-SVW-JEM
The Honorable Stephen V. Wilson, District Judge, Presiding

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFFS-APPELLANTS' PETITION FOR PANEL REHEARING OR REHEARING EN BANC

Saira Hussain
Sophia Cope
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: saira@eff.org
Telephone: (415) 436-9333

Counsel for Amicus Curiae
Electronic Frontier Foundation

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amicus curiae* states that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

Dated: October 12, 2023

By: /s/ *Saira Hussain*
Saira Hussain

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Rules

Other Authorities

STATEMENT OF INTEREST

The Electronic Frontier Foundation ("EFF") is a non-profit civil liberties organization with more than 34,000 dues-paying members that has worked for over 30 years to ensure that technology supports freedom, justice, and innovation for all people of the world. As an organization focused on the intersection of civil liberties and technology, EFF is particularly concerned with protecting the constitutional rights to free speech and digital privacy at a time when technological advances have resulted in the ability of the government to pry into the private lives and expressive activities of United States citizens and residents.

Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), *amicus* certifies that no person or entity, other than *amicus curiae*, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. Pursuant to Circuit Rule 29-2(a), the parties have consented to the filing of this brief.

INTRODUCTION

In the social media age, secrecy should not be a prerequisite for privacy. *See United States v. Jones*, 565 U.S. 400, 418 (2012) (Sotomayor, J., concurring). Over 75 percent of the world's population age 13 and older uses social media, with 4.74 billion people using social media worldwide.[1] Seventy-two percent of Americans use social media.[2]

Social media sites allow users to "engage in a wide array of protected First Amendment activity on topics as diverse as human thought." *Packingham v. North Carolina*, 137 S.Ct. 1730, 1735–36 (2017) (internal quotation and citation omitted). And when viewed comprehensively, such content can reveal vast amounts of users' personal details. To prying eyes, including those of the government, social media can be a gold mine for surveillance; indeed, as Justice Sotomayor recognized, "the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

---

[1] Claire Beveridge & Sam Lauron, *160+ Social Media Statistics Marketers Need for 2023*, Hootsuite (Jan. 26, 2023), https://blog.hootsuite.com/social-media-statistics-for-social-media-managers/.

[2] *Social Media Fact Sheet*, Pew Research Center (April 7, 2021), https://www.pewresearch.org/internet/fact-sheet/social-media.

That is what happened to Plaintiffs. Three federal government agencies—U.S. Customs and Border Protection ("CBP"), U.S. Immigration and Customs Enforcement ("ICE"), and the Federal Bureau of Investigations ("FBI")—created a wide-ranging surveillance program of activists, attorneys, journalists, and organizers for their perceived association with migrant caravans traveling through Central America and Mexico. Through open-source research of social media profiles and scrutiny of existing law enforcement databases, the government compiled massive amounts of personal, sensitive information about Plaintiffs and their First Amendment activity, including "records containing information about their political expressions, associations with other activists and humanitarians, organizational financial transactions, occupational histories, social media accounts, and other detailed biographical data." Rehearing Br. [ECF 58-1] 3 (cleaned up).

The panel erred, and created a conflict with this Circuit's uniform precedent, when it held that Plaintiffs lack standing to seek expungement of their compiled data. The unlawful collection and retention of such sensitive and personal information in violation of the First and Fourth Amendments is a concrete injury for which expungement is an appropriate form of relief because of the risk of what the government, or another party that gets access to this data, may do with it. Indeed, the compilation and storage of Plaintiffs' data in government databases creates a "credible threat" of future harm. *See 303 Creative LLC v. Elenis*, 143

S.Ct. 2298, 2308 (2023) (quoting *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 159 (2014)). This Court should grant Plaintiffs' petition for panel rehearing, or alternatively, rehearing en banc because whether expungement requires an injury greater than government collection and retention of sensitive data in violation of the Constitution is a question of "exceptional importance." *See* Fed. R. App. P. 35(a)(2).

ARGUMENT

I. PLAINTIFFS HAVE SIGNIFICANT PRIVACY INTERESTS IN THE PERSONAL INFORMATION THE GOVERNMENT COMPILED ABOUT THEM FROM PUBLIC SOURCES

Plaintiffs have significant privacy interests in the personal information the government collected about them in violation of the First and Fourth Amendments—including their "names, birthdays, social security numbers, occupations, addresses, social media profiles, and political views and associations." *See* Op. 19. This injury is sufficiently concrete to justify standing to seek expungement of the information, contrary to the panel's erroneous holding.[3]

That the government obtained Plaintiffs' personal information, in part, from publicly available or "open" internet sources such as social media profiles and

[3] *Amicus* supports Plaintiffs' argument in their rehearing petition that the panel erred when it "imported a privacy requirement into the concreteness analysis for constitutional claims." Rehearing Br. [ECF 58-1] 13. But should this Court agree with the panel that some privacy interest is required, Plaintiffs have met their burden on that front to establish standing.

news articles does not diminish Plaintiffs' privacy interests in their information. Yet the panel wrongly held otherwise. *See* Op. 5, 19–20. This Court must reject the panel's "cramped notion of personal privacy," especially because modern digital technology makes surveillance and data compilation easier and cheaper for the government, threatening "the individual's control of information concerning his or her person." *See U.S. Dept. of Justice v. Reporters Committee for Freedom of Press ("RCFP")*, 489 U.S. 749, 763 (1989).

A. Internet Platforms Provide the Government an Easy and Cheap Way to Compile Details About Users' Personal Lives

Modern digital technologies are unprecedented in that they can chronicle in persistent, exhaustive, and minute detail all aspects of individuals' lives. Social media platforms (and other internet sites) can publicly reveal—and thus the government can easily glean from them—vast amounts of personal information about users, both in terms of the volume and the intrusive nature of that information, implicating users' privacy interests.

Internet platforms host massive amounts of data. Even more than a cell phone's "immense storage capacity," *see Riley v. California*, 573 U.S. 373, 393 (2014), social media profiles have virtually unlimited storage capacity because

they live in "the cloud"—that is, in companies' ever-expanding server farms.[4] This is far *more* than what *Riley* contemplated for cell phones: "Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos." *Id.* at 394. *Riley* noted, for example, that "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions." *Id.* This and more are often publicly available on social media platforms like Instagram and Facebook.[5]

Additionally, similar to cell phones, social media profiles and other online sources contain personal information that can reveal, both directly and by inference, "a wealth of detail about [individuals'] familial, political, professional, religious, and sexual associations." *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). Social media's "time-stamped data provides an intimate window into a person's life," *see Carpenter v. United States*, 138 S.Ct. 2206, 2217 (2018), and

[4] Hive is Facebook's data warehouse, which had (in 2014) 300 petabytes of data and absorbed four new petabytes of data per day. Kit Smith, *53 Incredible Facebook Statistics and Facts*, Brandwatch (June 1, 2019), https://www.brandwatch.com/blog/facebook-statistics. Each petabyte is equivalent to one million gigabytes. By comparison, modern smartphones hold an average of 128 gigabytes of storage. Nick Steinberg, *How Much Storage (in GB) Do I Need In My Phone?*, Lifewire (July 10, 2022), https://www.lifewire.com/how-much-phone-storage-5272110.

[5] Instagram is a platform popular for sharing photographs publicly. It has over two billion monthly active users who upload over 1,000 photos per *second*. Muninder Adavelli, *Instagram Daily Active Users: How Many Use It Daily*, TechJury (July 27, 2023), https://techjury.net/blog/how-many-daily-active-users-on-instagram/.

even their personality.[6] Here, the government collected information reflecting Plaintiffs' "political views and associations," among other detailed information. *See* Op. 19. *See also* Pl. Reply Br. [ECF 41] 16–17.[7]

The unique characteristics of digital technologies, in addition to their storage capacities, enhance the privacy interests that Plaintiffs have in their social media and other publicly available online data. The compilation of previously uncompiled information is key.[8] Internet platforms "collect[] in one place many distinct types of information … that reveal much more in combination than any isolated record." *See Riley*, 573 U.S. at 394. Hundreds or thousands of social media posts, photos and videos, group memberships, and other online sources such as news articles and blog posts can collectively reveal much more about a person than a few discrete

---

[6] Gwendolyn Seidman, *What Can We Learn About People From Their Social Media?*, Psychology Today (Sept. 21, 2020), https://www.psychologytoday.com/us/blog/close-encounters/202009/what-can-we-learn-about-people-their-social-media.

[7] CBP has a broader social media surveillance program, as described in a Privacy Impact Assessment that CBP published seven years late, and suspiciously after the news story broke that elicited this lawsuit. Saira Hussain & Sophia Cope, *CBP's Social Media Surveillance Poses Risks to Free Speech and Privacy Rights*, EFF Deeplinks (Aug. 5, 2019), https://www.eff.org/deeplinks/2019/08/deep-dive-cbps-social-media-surveillance-poses-risks-free-speech-and-privacy.

[8] For example, CBP uses a digital tool to "link a person's Social Security number to their social media posts and location data." *See* Joseph Cox, *Homeland Security Uses AI Tool to Analyze Social Media of U.S. Citizens and Refugees*, Vice (May 17, 2023), https://www.vice.com/en/article/m7bge3/dhs-uses-ai-tool-babel-x-babel-street-social-media-citizens-refugees.

pieces of content.[9] It is "the power of compilations to affect personal privacy that outstrips the combined power of the bits of information…." *See RCFP*, 489 U.S. at 765. Social media and other online sources provide an unprecedented historical record about individuals such that "the retrospective quality of the data here gives [the government] access to a category of information otherwise unknowable." *See Carpenter*, 138 S.Ct. at 2218. Thus, Plaintiffs' privacy interests are "substantial" given "that in today's society the computer can accumulate and store information that would otherwise have surely been forgotten." *See RCFP*, 489 U.S. at 771.

Moreover, modern digital technologies "make long-term monitoring relatively easy and cheap" for the government. *See Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment). The panel here failed to recognize that surveillance of social media and other online sources—"by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may alter the

[9] The government can also obtain personal information from data brokers, which themselves aggregate data from social media posts, as well as public records and other sources, to tease out known and inferred facts about millions of Americans. *See* Justin Sherman, *How Shady Companies Guess Your Religion, Sexual Orientation, and Mental Health*, Slate (April 26, 2023), https://slate.com/technology/2023/04/data-broker-inference-privacy-legislation.html. CBP is "among a wide range of federal agencies known to purchase Americans' private data" from data brokers. *See* Dell Cameron, *How the US Can Stop Data Brokers' Worst Practices—Right Now*, Wired (Feb. 8, 2023), https://www.wired.com/story/fcra-letter-data-brokers-privacy-regulation/.

relationship between citizen and government in a way that is inimical to a democratic society." *See Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (citation omitted).

B. Plaintiffs Have Significant Privacy Interests in Their Publicly Available Personal Information

Plaintiffs have legitimate and significant interests in protecting their digital lives from government scrutiny, even when those lives play out in public internet posts. The panel, in holding that Plaintiffs lack standing to seek expungement, relied on the fact that the government collected data on Plaintiffs, in part, using public sources like social media. *See* Op. 5, 19–20. However, the Supreme Court has repeatedly held that the government's collection and compilation of publicly available personal information can implicate individuals' privacy interests. "A person does not surrender all [constitutional] protection by venturing into the public sphere." *Carpenter*, 138 S.Ct. at 2217.

In *RCFP*, the Court held that individuals have "significant" privacy interests in their criminal history summaries, i.e., "rap sheets," compiled by the FBI. *RCFP*, 489 U.S. at 767, 780 (holding that "rap sheets" fall within the law enforcement records privacy exemption of the Freedom of Information Act). This is despite the fact that items of data compiled in "rap sheets" are often publicly available from local jurisdictions. The Court sought to preserve the "practical obscurity" of the criminal history data—although it is public, it is hard to find across various

sources. *Id.* at 762, 780. The Court recognized that there are special privacy interests associated with the government's digitized compilations of disparate public data: "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information." *Id.* at 764.

The Court has extended this reasoning to other types of compilations of publicly available information. In *Jones*, the Court "recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements," including their movements in public. *Carpenter*, 138 S.Ct. at 2217. In *Carpenter*, the Court held that "[w]hether the Government employs its own [GPS] surveillance technology as in *Jones* or leverages the technology of a wireless carrier, … an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information]." *Id.*

Here, the government leveraged the technology of social media platforms and other online sources to engage in surveillance of Plaintiffs. The government compiled data on Plaintiffs using, in part, various public sources, some of which themselves *further* provide easily retrievable digital compilations of individuals' personal lives in words, photos, videos, and other data. Social media profiles may

reveal not just users' physical locations over time (whether through location stamps, textual declarations, or by implication via photos), as was at issue in *Jones* and *Carpenter*, but also myriad aspects of their personal lives.

If individuals have significant privacy interests in their "rap sheets," despite the individual data points being publicly available as in *RCFP*, then surely Plaintiffs here have significant privacy interests in the *non-criminal* personal details about them gleaned from publicly available online sources, including particularly sensitive details that reflect First Amendment-protected activity such as "political views and associations." *See* Op. 19. Justice Sotomayor identified the constitutional problem when the government acquires data that reflects "the sum of one's public movements," and has "recorded and *aggregated* [it] in a manner that enables the Government to ascertain, more or less at will, [a person's] political and religious beliefs, sexual habits, and so on." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (emphasis added).

The panel here further erred in dismissing Plaintiffs' privacy interests because it failed to recognize that much publicly available personal information about a person is not made public by that person *voluntarily*. For example, a social media user's contacts may publicly reveal information about the user without their

consent.[10] One study even found that it is possible to predict personal information about *nonusers* of social media based on personal data and contact lists shared by users.[11] As the study's author put it, "[t]he persistent trace of our online social interaction can slowly accumulate enough data to effectively diminish the decision power of an individual to keep personal information private."[12] Additionally, a social media user may share content that allows for unintended inferences. Studies have found, for example, that even when a user does not explicitly indicate the nature of their relationships on social media, romantic relationships[13] and sexual orientation[14] can reliably be inferred. Moreover, a person may inadvertently share their personal information in a public manner, due to the complexities and difficulties in navigating privacy settings, which vary widely across social media

[10] *See, e.g.*, Facebook Help Center, *Who Can Tag Me and How Do I Know If Someone Tags Me on Facebook?* ("Anyone can tag you in photos and other posts."), https://www.facebook.com/help/226296694047060/.

[11] David Garcia, *Leaking Privacy and Shadow Profiles in Online Social Networks*, Science Advances (Aug. 4, 2017), https://advances.sciencemag.org/content/3/8/e1701172.

[12] *Id.*

[13] Brady Robards & Siân Lincoln, *Making It "Facebook Official": Reflecting on Romantic Relationships Through Sustained Facebook Use*, Soc. Media + Soc'y (Oct. 12, 2016), https://journals.sagepub.com/doi/10.1177/2056305116672890.

[14] Carter Jernigan & Behram F.T. Mistree, *Gaydar: Facebook friendships expose sexual orientation*, First Monday (Sept. 22, 2009), https://firstmonday.org/ojs/index.php/fm/article/view/2611.

platforms. From organ donation[15] to word processing software,[16] studies show that most people do not change default settings.[17] Younger people are more likely to take advantage of available settings than adults over 50.[18] On some social media platforms, it can be difficult to discern exactly what information is public by default.[19] Particularly worrisome, some platforms change privacy settings without warning.[20]

While some individuals do understand that what they share on social media or other places online is public, they are still harmed when the government creates

---

[15] Shai Davidai, Thomas Gilovich & Lee D. Ross, *The Meaning of Default Options for Potential Organ Donors*, Proceedings of the Nat'l Acad. Sci. 109:38 (Sept. 18, 2012), https://pubmed.ncbi.nlm.nih.gov/22949639/.

[16] Jared Spool, *Do Users Change Their Settings?*, UIE (Sept. 14, 2011), https://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings.

[17] Venmo, the financial social media app, infamously makes transactions public by default. *See* Mia Sato, *Here's a Reminder to Make Your Venmo Transactions Private, Courtesy of Clarence Thomas*, The Verge (July 12, 2023), https://www.theverge.com/2023/7/12/23792922/venmo-transactions-privacy-security-risks-clarence-thomas.

[18] Mary Madden & Aaron Smith, *Reputation Management and Social Media*, Pew Research Center (May 26, 2010), https://www.pewresearch.org/internet/2010/05/26/reputation-management-and-social-media.

[19] *See, e.g., Add and Edit Your Profile Info*, Facebook Help Center (explaining how to change various settings without consistently explaining what information is public by default), https://www.facebook.com/help/1017657581651994.

[20] Will Oremus, *Facebook Changed 14 Million People's Privacy Settings to "Public" Without Warning*, Slate (June 7, 2018), https://slate.com/technology/2018/06/facebook-changed-14-million-peoples-privacy-settings-to-public-without-warning-due-to-a-bug.html.

an "all-encompassing record" of their personal lives. *See Carpenter*, 138 S.Ct. at 2217. The government's compilation of Plaintiffs' personal data from online sources is yet another example of why courts should "cease[] [to] treat secrecy as a prerequisite for privacy." *See Jones*, 565 U.S. at 418 (Sotomayor, J., concurring).

II. EXPUNGEMENT OF PLAINTIFFS' PERSONAL INFORMATION IS REQUIRED BECAUSE THE GOVERNMENT'S UNLAWFUL COLLECTION AND RETENTION OF IT POSES A SIGNIFICANT RISK OF FUTURE HARM

Not only did the panel err in failing to recognize the significant privacy interests Plaintiffs have in the personal information the government collected and retained about them, the panel also erred in stating, "[t]he evidence in this case does not show that the government is using *or will use* the records in the future to investigate plaintiffs or prevent them from crossing the border or that a third party *will obtain* the records *and use* them to plaintiffs' detriment." Op. 17 (emphasis added). The panel's analysis of the risk of *future* concrete harm was flawed for two reasons.[21]

First, requiring Plaintiffs to show that the government "will use" their stored personal information, or that third parties "will obtain … and use" it, is too high a

[21] *Amicus* agrees with Plaintiffs' argument that no additional risk of harm is needed beyond the unconstitutional collection and ongoing retention of their personal information. Rehearing Br. [ECF 58-1] 5, 10. However, to the extent this Court deems that standing for expungement requires something more, the government's retention of Plaintiffs' personal information poses a significant risk of future additional harm.

burden. Instead, the correct standard is whether the government's collection and retention of Plaintiffs' personal information creates a "credible threat" of future harm to Plaintiffs from using or disclosing that information. *See 303 Creative*, 143 S.Ct. at 2308 (quoting *Susan B. Anthony List*, 573 U.S. at 159).

Second, the panel recognized only a few of the many ways in which Plaintiffs' personal information could be used or disclosed in the future. Op. 17. Additional common uses and abuses of the data that would harm Plaintiffs include agency leaders identifying new ways to use the data or sharing it with other agencies, agency employees misusing the data without authorization, and thieves stealing the data during a breach. The government's breadth of intelligence collected about Plaintiffs, their indefinite retention of much of it, and the numerous examples of past injuries from data retained about others creates a significant risk of these harms sufficient to confer standing.

Data sharing across government agencies. The potential for ever-expanding interagency data sharing, followed by new forms of data usage, is a credible risk that justifies expungement. Although this surveillance program originated with three U.S. federal agencies, the evidence shows that they distributed Plaintiffs' personal information far beyond those agencies, for example

to Mexican law enforcement.[22] *See* Pl. Reply Br. [ECF 41] 6. The principal database the government used to store Plaintiffs' personal information had no rules about the kind of data that could be entered or for how long it could be retained. Pl. Opening Br. [ECF 20] 15. Even where limits existed on Plaintiffs' data, they imposed retention periods as long as 75 years,[23] and allowed liberal sharing with other agencies.[24] A quintessential example of harmful interagency sharing of personal information is the Census Bureau's provision of race and residence data—along with age, sex, citizenship, and country of birth—to the War Department, which used this information to carry out the internment of Japanese Americans during World War II.[25] Plaintiffs have significant privacy interests against further interagency sharing and use of their personal data.

---

[22] Dept. of Homeland Security Office of Inspector General, *CBP Targeted Americans Associated with the 2018-2019 Migrant Caravan*, 21 (Sept. 20, 2021), https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-62-Sep21.pdf.

[23] *See*, *e.g.*, Dept. of Homeland Security, *TECS System of Records Notice*, 77782 (Dec. 19, 2008) ("The retention period for information maintained in TECS is seventy-five (75) years…."), https://www.govinfo.gov/content/pkg/FR-2008-12-19/html/E8-29807.htm.

[24] *See id.* at 77779 ("TECS also allows direct access to other major law enforcement systems, including the Department of Justice's National Crime Information Center (NCIC), the National Law Enforcement Telecommunications Systems (NLETS), and the Canadian Police Information Centre (CPIC).").

[25] Stephen A. Holmes, *Report Says Census Bureau Helped Relocate Japanese*, N.Y. Times (Mar. 17, 2000), https://www.nytimes.com/2000/03/17/us/report-says-census-bureau-helped-relocate-japanese.html.

Employee misuse. The growing size and accessibility of law enforcement databases like those that house Plaintiffs' data have created opportunities for government employees to abuse these databases for their own personal gain. In 2013, for example, an internal NSA investigation revealed at least a dozen NSA employees[26] engaged in "unauthorized use of data about more than 3,000 Americans and green-card holders."[27] The pattern also holds at the local level. A 2016 *Associated Press* investigation based on public records requests found that the very databases that give officers critical information about people they encounter can be misused for purposes such as "voyeuristic curiosity," while in egregious cases, officers have "used information to stalk or harass, or have tampered with or sold records they obtained."[28] Plaintiffs not only have significant privacy interests in preventing the government from compiling their personal information in the first place, *see supra* Part I, but also in preventing government

[26] Alina Selyukh, *NSA Staff Used Spy Tools on Spouses, Ex-Lovers: Watchdog*, Reuters (Sept. 27, 2013), https://www.reuters.com/article/us-usa-surveillance-watchdog/nsa-staff-used-spy-tools-on-spouses-ex-lovers-watchdog-idUSBRE98Q14G20130927?feedType=RSS&feedName=domesticNews.

[27] Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, Wash. Post (Aug. 15, 2013), https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html.

[28] Sadie Gurman, *Across US, Police Officers Abuse Confidential Databases*, Assoc. Press (Sept. 28, 2016), https://apnews.com/699236946e3140659fff8a2362e16f43.

employees from accessing their personal information for inappropriate purposes. Expungement is the best way to ensure that government employees do not do so.

Data thieves. Data breaches are an endemic problem in modern life. A record 1,862 data breaches occurred in 2021, up 68% from the year prior, and far exceeding the previous record of 1,506 breaches in 2017.[29]

The government is not immune to such breaches. In 2019, a CBP subcontractor suffered a massive data breach of sensitive data, including face prints and license plate images, collected by CBP during a face recognition pilot program.[30] The subcontractor transferred copies of CBP's biometric data to its own network without the agency's knowledge, and that network was later the target of a malicious attack.[31] In a review of the incident, the DHS Inspector General identified CBP's information security practices as "inadequate to prevent the subcontractor's actions."[32] In total, over 100,000 traveler face prints and license

[29] Identity Theft Resource Center, *2021 Annual Data Breach Report*, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/.

[30] Sidney Fussell, *This Is Exactly What Privacy Experts Said Would Happen*, The Atlantic (June 11, 2019), https://www.theatlantic.com/technology/archive/2019/06/travelers-images-stolen-attack-cbp/591403/.

[31] Dept. of Homeland Security Office of Inspector General, *Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot*, 5 (Sept. 21, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

[32] *Id.* at 5–6.

plate images were compromised, and at least 19 were posted to the dark web.[33] This is far from the only example of CBP's poor data security practices.[34] Plaintiffs have significant privacy interests in preventing their data from disclosure in a breach, particularly because the information the government compiled includes highly sensitive information, such as Social Security numbers, *see* Op. 19, valuable to data thieves interested in conducting identity theft.[35]

CONCLUSION

For the reasons stated above, this Court should grant Plaintiffs' petition for panel rehearing, or alternatively, rehearing en banc.

Dated: October 12, 2023

Respectfully submitted,

By: /s/ *Saira Hussain*

Saira Hussain
Sophia Cope
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
saira@eff.org

Counsel for Amicus Curiae
Electronic Frontier Foundation

[33] *Id.* at 13.

[34] *See generally* Dept. of Homeland Security Office of Inspector General, *CBP Has Placed Travelers' PII at Risk of Exploitation* (July 15, 2021), https://www.oig.dhs.gov/sites/default/files/assets/2021-07/OIG-21-47-Jul21.pdf.

[35] *See, e.g.*, Brianna McGurran, *What Personal Information Can Be Used to Commit Identity Theft?*, Experian (July 31, 2022), https://www.experian.com/blogs/ask-experian/what-information-is-at-risk-for-identity-theft/.

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), I certify as follows:

1. This Brief of Amicus Curiae Electronic Frontier Foundation in Support of Plaintiffs-Appellants' Petition for Panel Rehearing or Rehearing En Banc with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 4,100 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 365, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: October 12, 2023

By: */s/ Saira Hussain*
Saira Hussain

Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on October 12, 2023.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: October 12, 2023

By: /s/ *Saira Hussain*
Saira Hussain

Counsel for Amicus Curiae